July 13, 2004 Draft

REGULATING INTERNET PAYMENT INTERMEDIARIES

Ronald J. Mann*

TABLE OF CONTENTS

---

* William Stamps Farish Professor in Law, University of Texas School of Law. I thank Allison Mann for inspiration, Mark Gergen, Clay Gillette, Stephanie Heller, Doug Laycock, Lynn LoPucki, Richard Markovits, Bob Rasmussen, Mark West, Jay Westbrook, and Jim White for comments, John Meline for graphics, and Bill Powers for unstinting support.

Abstract

This paper examines legal and policy issues raised by changes in payment methods related to the rise of the Internet. The two major changes – the rise of P2P systems like PayPal, and the rise of Internet billing systems (EBPP) to replace the use of paper bills and checks – both involve new intermediaries that facilitate payments made by conventional payment systems. The paper first discusses how those systems work. It then discusses problems in the framework currently used to regulate those systems in the United States, which has not been updated to protect consumers from the special problems those systems raise. Finally, the paper considers problems with the potential shift of payments services from the heavily regulated banking industry to new and unregulated Internet-related startups. The paper considers a variety of strategies for producing a level field of competition between banks and the new entities and at the same time providing adequate protection for the consumers that use the systems in question.

REGULATING INTERNET PAYMENT INTERMEDIARIES

I. INTRODUCTION

The Internet has produced significant changes in many aspects of commercial interaction. The rise of Internet retailers is one of the most obvious changes. Oddly enough, however, the overwhelming majority of commercial transactions facilitated by the Internet use a conventional payment system. Thus, even in 2002, at least 80% of Internet purchases were made with a credit card.[1] To many observers, this has come as a surprise. The early days of the Internet heralded a variety of proposals for entirely new payment systems – generically described as electronic money – that would use wholly electronic tokens that consumers could issue, transfer, and redeem. Years later, however, no electronic-money system has gained a significant role in commerce.[2]

The continuing maturation of the Internet, however, has brought significant changes to the methods by which individuals make payments. Person-to-person (P2P) systems like PayPal now make hundreds of millions of payments a year between individuals.[3] The most common purpose is to facilitate the purchase of items at Internet auctions, but increasingly P2P transfers are used to transfer funds overseas. Less far along, but gaining transactions rapidly, are a variety of systems for electronic bill

---

[1] The federal government does not collect official statistics about the use of various payment systems, so I necessarily rely on published estimates. Because those estimates often are based on survey data and similar sources, their accuracy is open to question. On this point, for example, assessments differ substantially. *See* Linda Punch, *Authentication's Tentative Gains*, CREDIT CARD MANAGEMENT, May 2002, at 26, 26 (reporting 90% without specifying the relevant time period); *Payment Instruments as a Percentage of Total eCommerce at* http://www.epaynews.com/statistics/transactions.html#45 (last visited Mar. 11, 2003) (reporting 81.3% for 2002). Those high rates of usage persist despite the widespread concern about the security of payments made by credit card. *See, e.g.*, *US Credit Card Fraud Statistics 2000-2007 at* http://www.epaynews.com/statistics/fraud.html#21 (last visited Mar. 15, 2003) [hereinafter *ePaynews Online Fraud Data*] (reporting rates of online credit-card fraud about three times as high as overall credit-card fraud rates).

[2] The most famous of the electronic-money providers, DigiCash, eventually filed for bankruptcy. For discussion of the reasons that electronic-money products have failed to make a market impact, see, *e.g.*, RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 491-97 (2002); Brian Mantel, *Why Don't Consumers Use Electronic Banking Products: Towards a Theory of Obstacles, Incentives, and Opportunities* 22-23 (Fed. Reserve Bk. of Chi. Emerging Payments Occasional Paper Series 2000-1) (Sept. 2000) *available at* http://www.chicagofed.org/publications/publicpolicystudies/emergingpayments/pdf/eps-2000-1.pdf (last visited Apr. 2, 2003).

[3] *See P2P Payment Provider Activity, 2001-2005 at* http://www.epaynews.com/statistics/transactions.html#45 (last visited Mar. 11, 2003) (reporting 105 million P2P payments in 2002 and predicting 1.4 billion P2P payments in 2005).

presentment and payment (EBPP).[4] Interestingly, both of those developments follow a path less ambitious than the still-hypothetical electronic-money systems: they involve the use of intermediaries to "piggyback" on existing systems to provide payment. Thus, in essence, they use the technology of the Web site to facilitate the use of conventional payment networks.[5]

However disparate those developments might seem at first glance, they present a common challenge to the regulatory system.[6] Unlike banks, which control the execution of payment transactions in conventional payment transactions, the intermediaries that populate these new sectors generally are not inevitably subject to regulatory supervision. At most, they are subject to regulation as money transmitters (akin to the regulation of Western Union).[7]

That circumstance presents a serious gap in the regulatory scheme. The pervasive regulatory supervision of banks helps to ensure that they honor their obligations under a variety of consumer-protection and data-privacy regulations that govern their activities.[8] A shift of a significant share of volume to the new and unregulated entities raises a corresponding risk of loss from the irresponsibility of those entities.[9] Thus, although the

---

[4] The market for online bill payment has the potential to be much larger than the P2P market. A recent Federal Reserve study, for example, indicates that consumers in 2000 wrote about 15 *billion* checks to make bill payments. *The Use of Checks and Other Noncash Payment Instruments in the United States*, Fed. Reserve Bull., Aug. 2002, at 361, 367 (reporting 42.5 billion checks, of which 36% were written by consumers for bill payments). Presently, about a quarter of Americans are using an EBPP product. *See* Cardflash, *E-Billing Projections* (Oct. 11, 2002 e-mail on file with author) (reporting that 22% of Americans would be using e-billing systems as of the end of 2002); *Percentage of US Households Actively Using Online Banking at* http://www.epaynews.com/statistics/bankstats.html#35 (last visited Mar. 11, 2003) (reporting that 24% of Americans used online banking actively in 2002 and that 27% are doing so in 2003).

[5] *See* Brian Mantel & Tim McHugh, *Changing E-Payment Payment Networks in the U.S.: The Strategic, Competitive & Innovative Implications* 2-9, *at* http://www.chicagofed.org/paymentsystems/publications/E-Payment_Networks_Mantel_McHugh.pdf (last visited Mar. 26, 2003) (discussing the general development of "product-independent payment networks").

[6] *See* Andrew L. Shapiro, *Digital Middlemen and the Architecture of Electronic Commerce*, 24 OHIO N.U. L. REV. 795, 801-05 (1998) (suggesting the need for new regulatory models to deal with Internet-based reintermediation).

[7] *See infra* notes 112-118 and accompanying text.

[8] For a discussion of those protections, see *infra* pp. 11-16.

[9] For one of several articles about problems targeting P2P systems, see, *e.g.*, Linda Rosencrance, *E-mail Scams Continue to Target PayPal Users* (Mar. 10, 2003) *at* http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,79222,00.html (last visited Mar. 11, 2003). For discussion of security problems in EBPP systems, see A. Andreeff et al., *Electronic Bill Presentment and Payment—Is It Just a Click Away?*, ECON. PERSP., 4th Qu. 2001, at 2, 10, *at*

risk of fraud and privacy violations is doubtless higher in these new forms of transactions than it is in conventional transactions, the regulatory framework is much weaker.[10]

Although the advent of the new transactions has been widely noted,[11] the literature contains no sustained legal or policy analysis of the problems that they pose. This paper responds to that challenge. The analysis proceeds in three steps. Part II provides a summary description of the mechanics of the systems, focusing on how they interact with existing payment systems and conventional actors in those systems. Part III explains the problems with the existing laws (principally the Electronic Funds Transfer Act (the EFTA) and regulations that the Federal Reserve has promulgated to implement that statute). Generally, the problem is that the outdated provisions of the EFTA and the applicable regulations leave consumers exposed to losses from fraud and error in the new transactions from which federal law would protect them if the transactions had been completed directly with conventional payment systems. Finally, Part IV examines broader questions of how to ensure that the new Internet intermediaries are adequately motivated to comply with whatever obligations the EFTA and privacy laws impose. Any regulatory intervention must accommodate both the benefits of increased competition from those new entities and the risks that their lack of responsibility will harm the consumers whose accounts are involved in the transactions.

II. THE NEW TRANSACTIONS

A. P2P Systems

The success of eBay's auction business[12] had the rare effect of creating a vast market for an entirely new payment product, one that would allow non-merchants (who cannot accept conventional credit-card payments[13]) to receive payments quickly in

---

http://www.billingforbusiness.com/issues/is%20it%20just%20a%20click%20away.pdf (last visited Mar. 11, 2003).

[10] *See supra* note 1 (referring to statistics about Internet payment fraud).

[11] Andreeff, *supra* note 9; Kenneth N. Kuttner & James J. McAndrews, *Personal On-Line Payments*, FRBNY ECON. POL'Y REV., Dec. 2001, at 35, *available at* http://www.newyorkfed.org/rmaghome/econ_pol/2001/1201kutt.pdf (last visited Mar. 26, 2003); Loretta J. Mester, *The Changing Nature of the Payments System: Should New Players Mean New Rules?*, BUS. REV. (Fed. Res. Bank of Phila.), MAR./APR. 2000, at 3; Ann H. Spiotto, *Electronic Bill Payment and Presentment: A Primer*, 57 BUS. LAWY. 447, 455-58 (2001); Ann Spiotto & Brian Mantel, *Rethinking Business: Electronic Bill Payment and Presentment and Aggregation*, ABA BANK COMPLIANCE, May/June 2001, at 18.

[12] *E.g.*, Brad Hill, *What Makes eBay Invincible* (Mar. 4, 2003) *at* http://www.ecommercetimes.com/perl/story/20900.html (last visited Mar. 11, 2003).

[13] Currently, there is no credit-card network in the United States with more than five million merchants that accept it. *See U.S. End-of-Year Merchant Acceptance by Brand - Current & Historical at* http://www.cardweb.com/carddata/charts/acceptance.html (last visited Mar. 11, 2003). Five million may be a lot, but it is only a few percent of the total population of the nation.

remote transactions.[14] Without such a system, purchasers in the early days of eBay had to use cashier's checks or money orders. Typically, sellers waited to ship products until they received the paper-based payment device in the mail. From a flood of startups offering competing products,[15] PayPal (now owned by eBay) has emerged as the dominant player in the industry,[16] now processing hundreds of millions of payments each year.[17] Indeed, industry sources expect that by 2005, auction payments will account for 95% of the possibly four *billion* person-to-person payment transactions expected to be made that year.[18] A separate (and much smaller) submarket, exemplified by CitiBank's c2it service, uses similar systems for cross-border payments.[19]

To understand the policy ramifications of P2P payments, it is necessary to understand the relation between the P2P provider and the conventional accounts from which and to which P2P payments are made. That relation can be illustrated by a summary of the three steps that must be completed for a successful P2P transaction.

1. Providing Funds for Payment

The purchaser that wishes to use a P2P provider to make a payment has two general ways to provide funds for payment. First, it could fund an account[20] with the

---

[14] *See* Kuttner & McAndrews, *supra* note 11, at 35.

[15] For a discussion of competitors in the heyday (around 2000), see Jesse Berst, *The Check's in the Mail: P2P Payments Come of Age* (Oct. 2, 2000), *at* http://www.zdnet.com/anchordesk/stories/story/0,10738,2635392,00.html (last visited Mar. 11, 2003) (discussing PayPal and eight competitors).

[16] For a discussion of the failed efforts by Amazon and Yahoo, see Hill, *supra* note 12.

[17] *See About Us at* http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside (last visited Mar. 11, 2003) (reporting twenty million registered users). PayPal's transaction volume increased by 80% during the last year, rising to $2.63 billion in the first quarter of 2003. *See* Email from CardFlash (Apr. 25, 2003) (copy on file with author).

[18] Lavonne Kuykendall, *Year Later, Little Payoff in Web P-to-P Payment*, AM. BANKER, Apr. 2, 2001, at 12. For a more pessimistic assessment (that there will be *only* 1.4 billion transactions in 2005), see *supra* note 3.

[19] *See, e.g., Citibank's c2it Goes Global With International Funds Transfer Capability* (May 22, 2001) *at* http://www.citigroup.com/citigroup/press/010522a.htm (last visited Mar. 17, 2003) (CitiBank press release describing availability of transfers to thirty countries); *Sending the Greenbacks Home*, HINDU BUS. LINE, Aug. 8, 2002 (Internet edition), *at* http://www.blonnet.com/catalyst/2002/08/08/stories/2002080800120200.htm (last visited Mar. 17, 2003) (discussing the market advantages of the service, particularly for immigrants sending money from the United States to their home countries). The interface for the service is at https://www.c2it.com/C2IT/International/selectcountryint.jsp (last visited Mar. 17, 2003). For discussion of PayPal's relative weakness at international transfers, see Tiernan Ray, *eBay's Secret Weapon* (Mar. 19, 2003) *at* http://www.ecommercetimes.com/perl/story/21037.html (last visited Mar. 26, 2003).

[20] To open an account with a P2P payment provider, a customer typically fills out a form at the provider's web site. Because funding into the system often will be accomplished from

provider, normally by drawing on a deposit account or a credit-card account. Because it ensures that funds are available for an immediate transfer, that process is common for those who make frequent purchases. P2P account balances also are common for frequent eBay sellers, who receive funds into their P2P accounts from those to whom they make sales. Alternatively, the purchaser could wait until the moment that it wishes to make a purchase. Again, it could choose at the time of payment to provide the funds in question by drawing on either a deposit account or a credit-card account. As discussed below, the choice between a credit card and a deposit account as a funding source has significant legal consequences to the user.

In either case, the fee structure is likely to discourage the use of credit cards, because the P2P provider incurs higher fees when it pays the interchange owed to the bank that has issued the credit card from which funds are drawn than when it pays the fees necessary to draw funds from a deposit account through a debit entry in the ACH system.[21] Similarly, because the P2P provider can profit by investing funds that remain in transaction accounts, some providers (including PayPal) encourage users to leave funds in those accounts by paying interest on them.[22]

2. Making Payments

The attraction of the P2P process, of course, is that it is quite simple to make payments. Normally, the only information that the purchaser needs to make a payment is the amount of money and the email address of the intended recipient. After entering that

---

some other account, that process is followed by some form of offline verification of the identity of the customer. That precaution is required because P2P systems have been the subject of frequent fraudulent attacks—both by organized crime groups trying to launder funds, *see, e.g.*, Beth Cox, *eBay to PayPal Gamblers: No Dice* (July 12, 2002), *at* http://siliconvalley.internet.com/news/article.php/1403631 (last visited Mar. 12, 2003); Ina Steiner, *eBay/PayPal Fraud with a Twist: International Money Laundering* (Jan. 29, 2003), *at* http://www.auctionbytes.com/pages/abn/y03/m01/i29/s01 (last visited Mar. 12, 2003), and by credit card thieves trying to extract immediate cash, *see* Evan I. Schwartz, *Digital Cash Payoff* (Dec. 2001) *at* http://www.technologyreview.com/articles/schwartz1201.asp (last visited Mar. 12, 2003).

[21] At PayPal, for example, personal accounts cannot accept credit-card payments. A user can accept those payments only by upgrading to a Premier or Business account. *Fees Policy* § b (Feb. 20, 2003) *at* http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_fees-outside (last visited Mar. 12, 2003) [hereinafter *PayPal Fees Policy*]. Those accounts are charged a schedule of fees starting at 2.2% for payments that they receive. *Fees for Receiving Payments (Premier and Business Accounts) at* http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fees-receiving-outside (last visited Mar. 12, 2003).

[22] *See* Ron Leuty, *PayPal Hunts for Steady Revenues*, SAN FRANCISCO BUS. TIMES, July 13, 2001, *available at* http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2001/07/16/focus5.html (last visited Mar. 12, 2003) (discussing the transition from a model in which PayPal made money "off the float" to a transaction-fee model, under which transaction fees are now 90% of PayPal's revenues).

information into a form at the P2P provider's Web site, the purchaser clicks on a "send money" button to request execution of the transaction. If the funds are sent from a balance in an account with the P2P provider or if they are drawn from a credit card, they should arrive in a few hours. If they are drawn directly from a deposit account, arrival will be delayed by a few days (until settlement of the ACH transaction to obtain the funds from the user's bank).[23]

3. Collecting Payments

The final step is for the recipient (the seller if the payment is for an auction) to collect the payment. In the typical process, the recipient receives an email notifying it that the payment has arrived.[24] If the recipient has an account with the P2P provider and is willing to leave the funds in that account, then it need do nothing further. If it does not have an account, or if it wishes to withdraw the funds, it will need to go to the provider's Web site and provide the necessary details.[25]

Ordinarily, the recipient will pay some fee to the provider for making the payment available. Those fees vary considerably, but a typical charge at PayPal would be 25-50 cents plus 2-4% of the transaction amount.[26] In addition, if the payment is made with a credit card, the recipient may be required to bear the cost of any chargeback that the payor seeks under its agreements with the provider and card issuer.[27]

---

[23] *See, e.g., Fees, Limits and Transaction Timeframes, available from* https://www.c2it.com/C2IT/Login (Fees, Limits and Transaction Timeframes tab) (last visited Mar. 12, 2003) [hereinafter *c2it Fees and Availability Schedule*] (setting out timeframe for when funds sent by c2it will be available).

[24] *See Making Payments – Send Money (Q: What happens after I send money?) at* http://www.paypal.com/cgi-bin/webscr?cmd=_help-ext&eloc=264&unique_id=01790&source_page=p/gen/ua/ua-outside (last visited Mar. 12, 2003) [hereinafter *PayPal Receive Money Procedures*].

[25] *See PayPal Receive Money Procedures*, *supra* note 24.

[26] *See supra* note 21 (discussing PayPal fee schedules).

[27] *See* User Agreement for PayPal Service § 5.1, *at* http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/ua-outside (last visited Mar. 12, 2003) [hereinafter *PayPal User Agreement*]. Those costs are likely to include not only the amount of the transaction, but also a chargeback fee imposed by the credit-card network (Visa or MasterCard, for example) in the range of $10. *See* PayPal Fees Policy, supra note 21, § e. If the chargeback occurs because the transaction turns out to be unauthorized, PayPal offers a Seller Protection Policy, under which PayPal will reimburse the seller for losses if the seller has behaved in a prudent manner when it shipped the goods to the buyer. *See Seller Protection Policy* (Feb. 11, 2003) *at* http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_spp-outside (last visited Mar. 12, 2003).

B. EBPP Systems

EBPP systems are at a much less mature stage in their development than P2P systems.[28] Accordingly, it is much harder to provide a clear picture of their operations. Generally, though, three different models compete within that industry. The first are products presented by the billing businesses, which send bills to consumers by email and provide a Web site at which payment can be made.[29] The second are products of depositary institutions, which permit their customers to pay bills at a Web site operated by the institution.[30] The third are offered by third-party intermediaries. The intermediaries operate Web sites that collect bills from various businesses, present them

---

[28] EBPP products gained a significant jump in usage during the anthrax scares in late 2001 – which at least temporarily raised consumer sensitivity to receiving and sending mail. *See* Keith Regan, *Report: Online Bill Payment Growing – Not Because of Mail Scares*, *at* http://www.ecommercetimes.com/perl/story/14718 (last visited Mar. 11, 2003) (discussing studies of spikes in EBPP usage about the time of the anthrax scares and suggesting that there is a long-term growth trend). The continuing growth during the years since then suggests that these products will continue to grow in importance during future decades. *See supra* note 4. Because growth appears to correlate with the availability of broadband Internet access, *see How Broadband Changes Consumer's Online Financial Activity at* http://www.epaynews.com/statistics/bankstats.html#23 (last visited Mar. 19, 2003) (reporting a survey indicating that broadband access is associated with a 46% increase in reviewing bills online and an 11% increase in paying bills online), the continuing growth of broadband access suggests that the market share of these products will continue to grow rapidly. *See* CheckFree, *Understanding EBP Models: Biller-Direct and Bill-Distribution* 4-5 (2001) (copy on file with author) [hereinafter CheckFree, *Understanding EBP Models*] (arguing that EBPP will grow in usage as more Americans are online). One recent survey estimates that about 28% of U.S. online households currently have broadband access and that the rate is growing at about 9% per month. *See Gartner Dataquest Survey Shows Steady Increase of Broadband Access in U.S. Households* (Nov. 13, 2002) *at* http://www3.gartner.com/5_about/press_releases/2002_11/pr20021113a.jsp (last visited Mar. 26, 2003).

[29] *See EBPP Share Between Banks, Billers & Third-Party Providers at* http://www.epaynews.com/statistics/bankstats.html#10 (last visited Mar. 11, 2003) [hereinafter *EBPP Share*] (reporting a 35% 2003 market share for the biller direct model); Steve Bills, *Card Issuers Poised to Profit in Electronic Bills*, AM. BANKER, June 11, 2002, at 8A, 9A (discussing the success of credit-card issuers using that model); Chris Costanzo, *E-Bill Presenters Meet Harsh Reality, See Hard Road Ahead*, AM. BANKER, May 22, 2002, at 1, 14 (discussing that model more generally). American Express alone has more than eight million customers who use that method of payment. *Online Account Management Figures For Banking & EBPP at* http://www.epaynews.com/statistics/bankstats.html#33 (last visited Mar. 11, 2003).

[30] Estimates for the market shares of the different models differ sharply, but it is clear that the bank-site model has a significant share of the market. *See EBPP Share*, *supra* note 29 (reporting a 20% market share for bank sites in 2003); Clare Saliba, *Study: Customers Like Banks for Online Bill Pay* (Nov. 12, 2001), *at* http://www.ecommercetimes.com/perl/story/14722 (last visited Mar. 11, 2003) (reporting a survey indicating that 55% of EBPP users use sites maintained by their bank).

to consumers on behalf of the billers, and then forward payment from the consumers to the billers.[31]

As with P2P systems, the fact that the different models compete to perform quite similar services for consumers should not obscure the significantly differing legal and policy implications of the different models. Accordingly, it is important to explain briefly how each of the three models works.

1. Biller Web Sites

As the name suggests, the biller Web site model is quite simple: the consumer goes directly to the biller's Web site to view the bill. In many cases, the site will "push" the bill to the consumer by sending an email that includes a link to the full details of the bill.[32] If the consumer is satisfied with the bill, it authorizes the biller to collect payment. The biller, in turn, proceeds to collect the payment (often through a third-party provider such as CheckFree).[33] Alternatively, the biller itself could initiate an ACH transaction debiting the consumer's account.[34]

As compared to conventional paper-based billing processes, those sites can save the substantial costs of preparing and mailing paper bills, as well as the costs of receiving and processing payments by mail.[35] There is likely to be a substantial reduction in the

---

[31] As with so many of the aggregate market statistics relevant to this subject, estimates differ sharply, but all show a significant share for third-party sites. *See EBPP Share*, *supra* note 29 (reporting a 45% market share for third-party sites in 2003); Saliba, *supra* note 30 (reporting a survey indicating that 10% of EBPP users use independent providers).

[32] For example, American Express offers a service that sends an email each month to its cardholders offering them a link to a place where they can view their monthly bill on the American Express Web site. *See* http://www.americanexpress.com/homepage/mt_personal.shtml (last visited Mar. 12, 2003) (button to "check and pay bill").

[33] *See* MURPHY & COMPANY, THE MURPHY & COMPANY EBPP EXECUTIVE REPORT 30 (2003) [hereinafter MURPHY REPORT]. CheckFree enters into contracts with a large number of billers and a large number of bill presentment sites of various kinds and routes the payments from the customers to the billers. For a description of the product, see the relevant portion of CheckFree's Web site at http://www.checkfreeisolutions.com/solutions/distribution_payment/index.html (last visited Mar. 27, 2003) (describing CheckFree's I-Processing Service).

[34] *See* Andreeff et al., *supra* note 9, at 7, 10 (discussing variety of payment options).

[35] Andreeff et al. estimate those savings at about $80 billion per year under traditional systems. Andreeff et al., *supra* note 9, at 2-3; *see also* Dawne Chandler, *Electronic Billing: Understanding the Road to Adoption* 2 (DST Output White Paper 2002), *at* http://www.output.net/docs/aboutus/ebilladoption.pdf (last visited Mar. 26, 2003); CheckFree, *Understanding EBP Models: Biller-Direct and Bill-Distribution* 2-3 (2001) (copy on file with author) [hereinafter CheckFree, *Understanding EBP Models*] (detailed discussion of cost savings); Steve Kille, *Leveraging Electronic Statement Delivery* 2 (Messaging Direct White Paper) (categorizing the various cost savings in detail), *available at*

costs of customer-support systems, as many inquiries can be shifted from the telephone to Web-site response systems.[36] Those sites also can have considerable marketing advantages, by enhancing the biller's ability to provide targeted advertising and by enabling the biller to develop more sophisticated customer profiles through the collection of information about bill-paying habits.[37] Many consumers also will view the systems as more convenient than traditional paper-based systems.[38] The biggest problem with those systems is the inefficiency of each consumer going to a separate site to pay each bill.

In the marketplace, those sites have been moderately successful, particularly for credit-card issuers.[39] Because the costs of the technology continue to decrease, there is good reason to think that more billers will offer such sites, as the number of customers necessary for the sites to break even falls.[40]

2. Internet Banking

When banks provide sites, they can overcome the biggest problem that biller Web sites face: the need for consumers to pay their bills site by site.[41] Thus, at the typical bank site, a consumer can pay any bill necessary, by entering onto a form at the site the information that the consumer has about the payment. Smaller banks are likely to

---

http://www.messagingdirect.com/publications/IC-6112.html (last visited Mar. 26, 2003); Lawrence J. Radecki & John Wenninger, *Paying Electronic Bills Electronically*, CURRENT ISSUES IN ECONOMICS AND FINANCE (Fed. Res. Bank of N.Y.), Jan, 1999, at 1, 2 (estimating costs at $20 billion).

[36] *See* IBM Global Services, *Electronic Bill Presentment and Payment: A Strategic Advantage* 2 (2000), *at* http://www-1.ibm.com/services/files/emea_final.pdf (last visited Mar. 26, 2003); MURPHY REPORT, *supra* note 33, at 93.

[37] *See* Andreeff et al., *supra* note 9, at 4; Chandler, *supra* note 35, at 2; IBM Global Services, *supra* note 36, at 3.

[38] Among other things, consumers can save the float caused by early payments, by facilitating payments that are made on precisely the date that the bill is due. They also can speed the payment process, if paying at the Web site is a few seconds faster than writing and mailing a check. *See* Andreeff et al., *supra* note 9, at 3-4; Chandler, *supra* note 35, at 1; IBM Global Services, *supra* note 36, at 4; Radecki & Wenninger, *supra* note 35, at 4. Those savings would amount to billions of dollars each year. *See* CheckFree, *Understanding EBP Models*, *supra* note 35, at 2-3 (detailed discussion of cost savings); MURPHY REPORT, *supra* note 33, at 1.

[39] For example, one study estimates that 74 percent of e-billers were using their own sites by the end of 2000. *See* Andreeff et al., *supra* note 9, at 6.

[40] Advances in information technology have lowered those costs substantially, so that a new system now could be set up for about $25,000 – and pay for itself in just a few years with as few as 3,000 customers. *See* MURPHY REPORT, *supra* note 33, at 69.

[41] CheckFree estimates that the "trigger" to induce the typical online consumer to use a consolidated presenter would be if the presenter could deliver five bills per month electronically. CheckFree, *Understanding EBP Models*, *supra* note 35,, at 6.

outsource all of the payment functions to a third-party provider like CheckFree.[42] Larger banks, however, may arrange the payments themselves in whatever manner is most cost-effective. For example, if the recipient is a major biller (such as a local utility), the bank may aggregate payments in a batch and pay them with a single ACH transaction. For isolated transactions, the bank might even cut a paper cashier's check and mail it to the recipient. Those sites have been particularly successful in recent years. One possible reason is that consumers are more willing to trust the necessary financial information to a bank at which they have a depositary relationship than to a third party billing them for a payment.

Another advantage, particularly by comparison to the third-party sites discussed below, is the simplicity of operation. The bank already would be involved in the payment transaction – whatever type of site the consumer used – but use of the bank's site obviates the need for involvement of an extra party. Also, many bank sites do not undertake to present bills electronically. Rather, they simply provide an easy method for consumers to pay the bills that are delivered to them by conventional means. Thus, they avoid the complications attendant on electronic presentation of bills,[43] which is a common feature of the two competing models. Of course, that may not be an advantage if consumers desire the functionality available from bill presentment. Thus, it is no surprise that bank sites increasingly offer bill-presentment services.

3. Third-Party Providers

The most ambitious systems are Web sites operated by third parties at which consumers can view and pay all (or almost all) of their bills. The promise of those sites is a future of a single integrated portal, through which all bills will be sent to a consumer and at which the consumer will be able to pay all bills.[44] The logistical problems of operating such a site are daunting. For one thing, the intermediary operating such a site (CheckFree, for example) must reach agreements with a large number of billers allowing it to present bills on their behalf and establishing a standardized data format for the information in those bills.[45] At the same time, the intermediary must persuade enough consumers to use the site to justify the fixed costs of developing the site's technology.

---

[42] *See supra* note 33 (discussing CheckFree's product).

[43] Many consumers have found those services to be too cumbersome. *See* Andreeff et al., supra note 9, at 8.

[44] Teri Robinson, *Time to E-Pay the Bills* (Oct. 23, 2000) *at* http://www.internetweek.com/indepth/indepth102300-1.htm (last visited Mar. 26, 2003).

[45] In recent years, CheckFree has become one of the leading players. http://www.checkfree.com (last visited Mar. 27, 2003). As discussed *supra* note 33, CheckFree – in addition to its own site – operates a significant network providing payment services to billers and banks that operate their own sites. The United States Postal Service and Paytrust were significant early players in the area. http://www.usps.com/money/welcome.htm?from=homedoorwaybar&page=0016money (last visited Mar. 12, 2003); http://www.paytrust.com (last visited Mar. 12, 2003).

Without a critical mass of billers and consumers, the site cannot prosper. This is, of course, a standard problem of bandwagon effects.[46]

When a consumer uses such a site to pay a bill, the process operates much as it does at a bank Web site. The consumer identifies the appropriate bill and authorizes payment. The intermediary, in turn, arranges for the payment to be sent to the biller, normally through an ACH debit entry from the consumer's deposit account.

For billers that do not operate their own site, these sites offer a significant benefit because of the potential for the cost savings that come from electronic presentation of bills (discussed above as a benefit of biller Web sites). But the cumbersome nature of the technology to date has made progress slow. Still, if they can overcome technical problems, they could ultimately becomethe dominant model. [47]

III. DESIGNING A SOUND REGULATORY SYSTEM

The first question in assessing the adequacy of regulatory protections for the developing Internet payment transactions is to assess the extent to which the consumer protections that apply to existing transactions extend to the new transactions. Two forms of consumer protection are relevant here: information privacy and protection from losses related to fraud or error.

The simpler of those relates to information privacy. Specifically, under Gramm-Leach-Bliley (GLB), "financial institutions" must not disclose nonpublic personal information to third parties unless they have given their customers an opportunity to opt out of any such disclosures.[48] Some might criticize the narrowness of that protection.[49] It is much narrower, for example, than protections afforded European consumers under the EU's Data Protection Directive and the statutes that implement it.[50] For present

---

[46] *See generally* JEFFREY H. ROHLFS, BANDWAGON EFFECTS IN HIGH-TECHNOLOGY INDUSTRIES chs. 3-4 (2001).

[47] There is a consensus that the third-party provider model has the potential to provide the most sophisticated aggregation of bills from a large set of providers. *See* Andreeff et al., *supra* note 9, at 9. On the other hand, it is not clear whether those providers will be able to convince enough customers and billers to join their systems to gain a major long-term role in the market. *See* Andreeff et al., *supra* note 9, at 9. Indeed, the most likely outcome probably is that providers of all three types will survive. *See* MURPHY REPORT, *supra* note 33, at 43.

[48] 15 U.S.C. § 6802(a) (financial institutions "may not * * * disclose to any nonaffiliated third party any nonpublic personal information, unless such financial institution provides * * * notice").

[49] For a general introduction to Gramm-Leach-Bliley, including a discussion of some of the most prominent criticisms, see MANN & WINN, *supra* note 2, at 156-60.

[50] See MANN & WINN, *supra* note 2, at 184-93.

purposes,[51] however, what is important is that a broad definition of "financial institution" in the applicable regulations means that the rules in GLB apply with just as much force to the new intermediaries as they do to banks and other depository institutions.[52]

It is much more complicated to assess the legal framework that protects consumers from fraud and error, because that framework plainly does not extend completely to the new payment intermediaries. To explain the problems with that framework, the sections that follow summarize the existing framework – and the policy choices that it reflects – and how those rules apply to problems likely to arise in the new transactions.

A. Existing Protections Against Fraud and Error

The most general protection for consumers in these transactions comes from the EFTA and Regulation E (which the Federal Reserve has promulgated to implement the EFTA). The EFTA/E regime applies to any electronic funds transfer (EFT).[53] The statute broadly defines that term to include not only Internet-initiated transactions, but also transactions at an automatic teller machine (ATM) and retail transactions that use a debit card to draw directly on a deposit account.[54] For any such transaction, the statute generally protects consumers[55] from losses caused by an unauthorized transaction. Thus, if a consumer loses a debit card, the consumer's bank would be obligated to restore to the consumer's account any funds removed for transactions that a thief made with the card. There are two important exceptions. First, the bank can charge the account a deductible of up to $50 for each series of unauthorized transactions.[56] Second, more importantly, the bank can charge the consumer more – and in some cases the entire amount of the losses – if the consumer does not advise the bank with sufficient promptness after the consumer learns that the card has been stolen.[57] The EFTA/E regime also provides a

---

[51] Part IV considers the concern that the payment intermediary might comply with its privacy obligations less reliably than a traditional depositary institution.

[52] *See* 16 C.F.R. § 313.3(k)(2)(vi) ("A business that regularly wires money to and from consumers is a financial institution * * * ."). For similar conclusions, see MURPHY REPORT, *supra* note 33, at 109; Jeffrey P. Taft, *Internet-Based Payment Systems: An Overview of the Regulatory and Compliance Issues*, CONS. FIN. L.Q. REP., Winter 2002, at 47.

[53] *See, e.g.*, EFTA §§ 905-907 (all referring to "electronic fund transfers").

[54] EFTA § 903(6); Regulation E § 205.3(b).

[55] For purposes of the EFTA and Regulation E, a consumer is any "natural person." EFTA § 903(5); Regulation E § 205.2(e).

[56] EFTA § 909(a); Regulation E § 205.6(b).

[57] EFTA § 909(a); Regulation E § 205.6(b).

detailed dispute-resolution process for resolving claims of errors by the financial institution in charging a consumer's account for a funds transfer.[58]

For credit-card transactions, analogous protections come from the Truth-in-Lending Act (TILA) and Regulation Z (which the Federal Reserve has promulgated to implement TILA). There are, however, important differences between the two regimes. For one thing, the TILA/Z regime provides broader protection for unauthorized losses – consumer responsibility is capped at $50 even if the consumer fails to notify the bank that the card has been stolen.[59] Also, the TILA/Z regime grants consumers[60] a broad right to withhold payment even for authorized transactions if the seller fails to perform as agreed.[61] As discussed below, the right to withhold provides consumers an important protection against seller fraud.

To the extent that the EFTA/E and TILA/Z regimes are justified, they rest on a series of contestable premises about the ways in which consumers interact with financial institutions. Among other things, they are in tension with the possibility that rational consumers and financial institutions would develop superior methods of allocating the risks and opportunities related to their commercial interactions. Bob Cooter and Ed Rubin have provided the most careful analysis of that problem, identifying a series of defects in the market in which consumers contract with financial institutions.[62] Perhaps the most persuasive of their points undermines the idea that consumers make informed choices about the relevant terms when they contract with financial institutions. As Cooter and Rubin explain, the rational individual consumer will not expend the time and effort to identify and understand the specific terms of the account agreement with its financial institution.[63] In contrast, the rational financial institution would expend considerable effort in formulating an agreement that furthered the bank's interests.[64]

---

[58] Among other things, that process requires the institution to return disputed funds to the consumers account within ten business days of receiving notice of the problem if it cannot complete an investigation of the matter by that date. EFTA § 908; Regulation E § 205.11.

[59] TILA § 133; Regulation Z § 226.12(b).

[60] The definition of "consumer" under TILA and Regulation Z is narrower than the definition in the EFTA/E regime, discussed *supra* note 55. It applies only to a natural person and also only if the funds in question are advanced "primarily for personal, family, or household purposes." TILA § 103(h); Regulation Z § 226.2(11) & (12).

[61] TILA § 170; Regulation Z § 226.12(c).

[62] *See* Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEXAS L. REV. 63, 68 (1987).

[63] *See* Cooter & Rubin, *supra* note 62, at 68-70.

[64] *See* Cooter & Rubin, *supra* note 62, at 80-81.

Thus, there is little reason to think that market pressures are driving the terms of consumer deposit-account agreements to an efficient norm.[65]

A second problem with those rules – as they apply to the conventional credit-card and debit-card transactions for which they are designed – is that the rules erect distinctions that are difficult to justify as a policy matter. It is easy to accept a distinction between the rules for near-cash transactions with debit cards and the rules for borrowing transactions executed with credit cards. Thus, a merchant that insists on taking cash justifiably might expect the law to accord more finality to the transaction than a merchant that accepts a device as unlike cash as a credit card.

But the differences between the EFTA/E and TILA/Z regimes do not map well to that common-sense transactional distinction. For example, a merchant that accepts a promissory note obviously has less certainty of final payment than one that accepts cash, primarily because of the practical likelihood that the purchaser/borrower may choose not to pay – an option not available to the cash purchaser. In the conventional credit-card transaction, however, the card issuer by contract with the merchant agrees to accept the risk that the cardholder will fail to pay balances charged on the card for reasons other than assertion of a defense to payment.[66] The TILA/Z regime discussed above effectively deprives the merchant of the possibility of making that contract – because any claim of a defect by the consumer will result in an immediate charging of the transaction back to the merchant.[67]

It is easy to see why that right is useful to consumers. And there are substantial policy reasons that can be adduced to support it. For example, merchants might have greater economies of scale and experience in conducting litigation than consumers. If so, placing the burden of litigation on the merchant by putting the money in the hands of the consumers when the dispute begins might produce results that are more equitable by offsetting the merchant's advantages.

But what is not clear is why it is appropriate for that rule to extend to credit-card transactions but not to debit-card transactions. The difficulty in justifying the distinction

---

[65] The market defects that Rubin and Cooter identify are just as likely in the electronic context as they are in the conventional banking context. *Cf.* Kuttner & McAndrews, *supra* note 11, at 42 (doubting that consumers are aware of the legal regime that governs P2P payments).

[66] *See* RONALD J. MANN, PAYMENT SYSTEMS AND OTHER FINANCIAL TRANSACTIONS: CASES, MATERIALS, AND PROBLEMS 112-16 (2d ed. 2003).

[67] To be sure, it does so indirectly – because the TILA/Z regime directly imposes responsibility for those defenses only on the issuer. But the effect is certain nonetheless, because of the pervasive credit-card network rules under which such claims are charged back to the merchant as soon as the customer makes them. *See* MANN, *supra* note 66, at 112-16. Moreover, it appears that the applicable dispute-resolution systems are designed to further the interests of issuers rather than merchants (or the institutions that process transactions for them, commonly known in the trade as "acquirers"). My discussions with industry professionals suggest that they generally are regarded as biased in favor of the cardholder.

only grows with the continuing convergence in the functions of the two products. For one thing, roughly 40% of consumers use the credit card entirely as a convenience device, repaying their bill each month in its entirety.[68] Why should their transactions have some special protection solely because of the possibility that they could choose not to pay for the transactions before interest began to accrue? Similarly, as more and more merchants accept debit cards at the point of sale, is it plausible as a policy matter that a consumer's right to withhold payment should depend on which particular piece of plastic the consumer swipes through the payment terminal? Cutting the point even more finely, with the advent of cards that include both credit and debit features, it is even harder to justify the availability of the right to withhold payment turning on the way in which the consumer interacts with the merchant's payment terminal (especially if that terminal is specifically designed to lead the consumer to choose the debit option rather than the credit option that would give the consumer a greater withholding right).[69]

Finally, several of the distinctions in the details between the TILA/Z and EFTA/E regimes can be explained by nothing other than differences in the level of concern for consumer in the differing Congresses that enacted them.[70] For example, what policy basis justifies the differing definitions of consumers in the two systems,[71] the differing protections for unauthorized transactions,[72] and the differing definitions of billing errors from which consumers are protected?[73]

From a broad perspective, the incoherence of those distinctions suggests that the system would be improved by a general articulation of a set of general legal rules to govern consumer payment systems. Those rules presumably would eradicate many of the distinctions that current law draws between functionally similar payment systems. At the same time, they plausibly might include distinctions between face-to-face and remote

---

[68] *See Bank Credit Card Convenience Usage – Current at* http://www.cardweb.com/carddata/charts/convenience_usage.amp (last visited Mar. 12, 2003).

[69] Interestingly, the main justification for the interface design is the lower interchange merchants pay for debit-card transactions than for credit-card transactions, *not* the greater rights the customers obtain in the credit-card transactions. *See* David Breitkopf, *PIN-Signature Debit Tug-of-War Escalates*, AM. BANKER, FEB. 25, 2002, at 6 (discussing the conflicting interests of merchants and customers, which prefer PIN-based debit, and banks, which prefer signature debit).

[70] I owe this explanation to Bob Rasmussen, which I adopt for lack of a better one of my own. *See also* Cooter & Rubin, *supra* note 62, at 91 (attributing some differences to "pure guesswork and political necromancy").

[71] Compare *supra* note 60 (discussing the definition of "consumer" in the TILA/Z regime) with *supra* note 55 (discussing the definition of "consumer" in the EFTA/E regime).

[72] Compare *supra* note 59 (discussing unauthorized transaction rules in the TILA/Z regime) with *supra* note 57 (discussing unauthorized transaction rules in the EFTA/E regime).

[73] Compare TILA § 161(b) (defining billing error to include, among other things, any transaction for "goods or services * * * not delivered to the obligor * * * in accordance with the agreement made at the time of a transaction"); Regulation Z § 226.13 (same) *with* EFTA § 908(f) (much narrower definition of "error"); Regulation E § 205.11(a) (same).

(telephone, mail-order, and Internet) transactions. For current purposes, however, the distinctions are important not because of the possibility that some future legislature might remove them. They are important to this project because they have been carried over into the Internet payment transactions on which this paper focuses – with no more coherence in that context than they have in the context where those distinctions developed.

B. Protections Against Fraud and Error in the New Transactions

Unfortunately, the legal framework protecting consumers against fraud and error has not been updated to accommodate the new transactions. Thus, that framework includes three types of problems: situations where the incoherent distinction between the TILA/Z and EFTA/E regime is replicated in the new environment, minor oversights in regulatory drafting, and more significant omissions in regulatory coverage. The sections below discuss how those rules apply to the new transactions, underscoring those problems where they arise.

1. P2P Transactions

Current experience suggests that fraud is a serious problem in P2P transactions. One Federal Reserve researcher, for example, estimates that PayPal's fraud rate of 0.66%, albeit much lower than the rate of online credit-card fraud, is about four times the rate of fraud for retail credit-card transactions and more than sixty times the rate for retail debit card transactions.[74] The legal rules for determining whether the consumer bears the losses from that fraud, however, depend in an important way on how the consumer pays for the transaction. To see the point, imagine an eBay auction in which a fraudulent seller never ships any goods to the buyer.[75] If the transaction is funded from the purchaser's account with the P2P provider, it is an EFT governed by the EFTA.[76] In that event, the purchaser has no right – as against the financial institution or the P2P provider – to recover the funds for an authorized transaction solely because of a complaint about misconduct by the seller, however meritorious the complaint. The same analysis applies if the purchaser funds the transaction by authorizing a transfer directly from the purchaser's deposit account: that also leads to an EFT covered by the EFTA/E regime.[77]

---

[74] *See* Tim McHugh, *The Growth of Person-to-Person Electronic Payments*, CHICAGO FED LETTER, Aug. 2002, *available at* http://www.chicagofed.org/publications/fedletter/2002/cflaug2002_180.pdf (last visited Mar. 26, 2003).

[75] The situation is not hypothetical. *See, e.g.*, *Scam Casts Doubt on eBay's Anti-Fraud Software* (Mar. 25, 2003), *at* http://www.siliconvalley.com/mld/siliconvalley/5450291.htm (last visited Mar. 26, 2003) (discussing a recent scam in which an Arizona couple stole $100,000 from more than 500 bidders).

[76] Section 903(6) of the EFTA defines an "electronic fund transfer" as a "transfer of funds * * * initiated through an electronic terminal * * * so as to * * * authorize a financial institution to debit or credit an account." *See* Regulation E § 205.3(b) (similar definition).

[77] *See supra* note 76 (quoting the relevant statutory language).

But if the buyer has the good luck (or foresight) to fund the purchase directly from a credit card, the transaction is governed instead by the TILA/Z regime. Among other things, that means that the purchaser would have the right to withhold payment if the seller in fact never supplies the goods.[78] As discussed above, it is odd to have such an important protection turn on something that is as trivial to the transaction as the method by which the purchaser funds the transaction to the P2P provider. It is not, however, any more odd to see that distinction here than it is to see it in the conventional point-of-sale context.

The other likely type of fraud is for a third party to obtain the consumer's PayPal login information and use that information to conduct an unauthorized transaction by drawing on the consumer's PayPal account.[79] If the interloper draws directly on the P2P account, Regulation E makes the P2P intermediary directly responsible: subject to the normal exceptions, the P2P provider cannot charge the consumer's account for the transaction. The same result applies under the TILA/Z regime if the interloper uses the information to draw funds from the consumer's credit card.

The only ambiguity applies if the interloper uses the information to withdraw funds from the consumer's deposit account. In that event – because of an odd glitch in the regulation – it seems that neither the P2P provider nor the bank is obligated to return the funds to the consumer's deposit account. The bank apparently is not obligated, because it is entitled to treat the transaction as authorized – a transaction is authorized under the EFTA if it is executed by a party (the P2P provider in this case) to whom the consumer has given the relevant access information.[80] Because that fact makes the transaction "authorized" with respect to the account from which funds were drawn, it appears that the rules related to "unauthorized" transaction impose no obligation on the P2P provider for the loss. The most likely source of recovery for the consumer would be an action against the P2P provider's depositary institution (the entity that originated the ACH transfer) for a breach of the applicable NACHA warranties.[81] Because of the

---

[78] In the framework of the statute, the bank attempting to collect the credit-card bill would be subject to the defense that the PayPal purchaser never received the goods it purchased. *See supra* note 61 and accompanying text (discussing the TILA/Z right to withhold payment).

[79] That is the point of some of the most prominent recent schemes directed at PayPal customers. *See* Alorie Gilbert, *PayPal Users Targeted by Email Scam* (Mar. 10, 2003) *at* http://news.zdnet.co.uk/story/0,,t269-s2131645,00.html (last visited Mar. 12, 2003) (discussing a recent scam involving emails fraudulently purporting to be from PayPal).

[80] *See* EFTA §§ 903(2) (defining "accepted card or other means of access"), 903(11) (defining "unauthorized electronic fund transfer"); Regulation E §§ 205.2(a)(1) (defining "[a]ccess device"), 205.2(m) (defining "[u]nauthorized electronic fund transfer").

[81] *See* NACHA Rules § 2.2.1.1 (warranty of authorization by the Originator of an ACH transfer); *see also* MANN, *supra* note 66, at 157-65 (general discussion of the ACH system and the legal framework that governs it).

limited litigation to date in that area, it is difficult to assess the likelihood of prevailing in such an action.[82]

That problem, however, is not a serious one. Unlike the incoherent boundary between the EFTA/E and TILA/Z regimes – which is a somewhat more permanent feature of our system – this problem seems to be a simple glitch, which the Federal Reserve easily could remedy on its own volition.[83]

2. EBPP Transactions

Because of the variety of business models, it is difficult to provide a comprehensive schema of the types of transactions that pose risks for consumers. One simplifying factor, however, is the general absence of credit-card payments from those transactions. What that means is that the legal issues focus almost entirely on the reach of the EFTA/E regime,[84] rather than its boundary with the TILA/Z regime. The simplest approach is to look separately at the risks posed by each of the three prevailing business models.

(a) Biller Web Sites

The most likely difficulty is an unjustified payment to the biller: the biller might pay one consumer's bill from another consumer's account or it might pay itself for a bill even if the consumer in fact did not authorize payment. Interestingly enough, the EFTA/E regime would not provide protection in either case. As discussed above, the consumer cannot claim that the transactions are "unauthorized" for purposes of the

---

[82] The limited cases to date suggest that all parties to the transaction arguably have a claim for breach of that warranty. *E.g.*, *Security First Network Bank v. C.A.P.S., Inc.*, 2002 WL 485352 (N.D. Ill. 2002) (permitting suit by victim of fraud against bank that executed unauthorized ACH transfers; discussing earlier cases).

[83] One simple response would be to add a new subsection 205.14(c)(3) stating as follows:

> Any unauthorized transaction that results in the removal of funds from the account at the financial institution will constitute a billing error for purposes of Section 205.11(a)(1), for which the payment service provider is responsible under Section 205.14(a), if the transaction involves the use either of (A) the access device issued by the payment service provider to the customer or (B) the access device provided by the consumer to the payment service provider for the account at the financial institution.

Because Section 205.14(c)(2) plainly implements the error-resolution procedures as against the payment service provider, the proposed subsection would ensure that the provider is obligated to restore funds to the consumer's account at the consumer's bank just as quickly as the bank would have to restore funds for a traditional unauthorized transaction.

[84] *See* Regulation E Official Staff Commentary § 3(b)-1(vi) (including within the definition of electronic fund transfer "payment made by a bill payer under a bill-payment service available to a consumer via computer or other electronic means").

EFTA/E regime.[85] For similar reasons, the consumer cannot claim that they amount to an "error." The statutory definition of "error," albeit vague, is directed to errors by the bank, not errors by a third party to whom the consumer has granted access.[86] Thus, the statute offers the consumer no recourse in that situation. Perhaps the situation is not unduly troublesome – given the likely solvency of the typical billing entity – but it does seem inconsistent with the general philosophy of the EFTA/E regime as applied to conventional transactions.

(b) Internet Banking

The framework for Internet banking is the simplest. Because there is no intermediary,[87] the financial institution takes all actions regarding the account. Accordingly, the rules in the EFTA/E regime apply directly to protect the consumer from unauthorized transactions and errors.

(c) Third-Party Providers

As the discussion above suggests, the harshest results for consumers come from the third-party systems, where the insertion of an intermediary enhances the likelihood that the EFTA/E regime will not apply. Two general problem transactions are apparent:

(I) Interloping and Erroneous Bills

In this scenario, a malefactor fabricates a bill and has the provider send it to the consumer. Alternatively, and less maliciously, the bill is a legitimate one that, because of an error by the intermediary, is posted and distributed to the wrong consumer. Then, suppose that the consumer pays the fraudulent or erroneous bill. For the reasons discussed above, the consumer will not be able to claim that the transaction is either unauthorized or a remediable error.[88] Of course, in this particular transaction it is easy to fault the consumer for not detecting the spoofed bill. But in many of the existing cases of Internet fraud, a consumer of ordinary sophistication would not necessarily have recognized the problem. Imagine a bill purporting to come from your local electric utility, in a format visually identical to the electric bill you receive every month, which arrives 29 days after your last bill and is in an amount approximately equal to that bill. Your first hint of a problem is likely to come when the legitimate bill appears the next day. Given that problem (a variation on the new Internet crime called "phishing"), it is

---

[85] *See supra* note 80 and accompanying text.

[86] EFTA § 908(f)(2).

[87] As discussed *supra* note 33, there might be an intermediary (such as CheckFree) between the bank and the payee, but that is irrelevant to the concerns of this paper, because there would be no intermediary between the consumer and the institution that holds the consumer's deposit account. To put it another way, it is plain that Regulation E would protect the consumer from mistakes by CheckFree operating as an intermediary between the bank and the payee.

[88] *See supra* notes 80, 86, and accompanying text.

reasonable to consider whether intermediaries should bear those losses. If they were responsible for those losses, they might be better motivated to develop technology to detect such infiltrations.[89] For present purposes, the important point is that the existing legal rule for this situation reflects pure happenstance rather than a reasoned resolution of the economic and policy issues.

(II) Interloping Payments

In this scenario, the intermediary makes a payment based on an instruction from an interloping malefactor rather than the consumer. As with the analogous P2P transactions, the ambiguity in the regulation's coverage of unauthorized transactions leaves a substantial possibility that the consumer has no protection.[90]

3. Summary

Although the discussion in the preceding sections might seem unduly detailed, the level of detail is important to show how difficult it is to design a system to govern the transactions in question. Neither the EFTA nor Regulation E is particularly old. Nor are they supervised by a regulatory agency out of touch with the developments in these transactions – many of the most informative papers in the area are written by Federal Reserve staff,[91] particularly by members of the group studying emerging payments in its Chicago branch. The point, however, is that these transactions are developing so rapidly and with such fertile inventiveness that it is difficult to expect any regulatory system to keep pace and ensure coherent coverage as long as the system is premised on the categorical distinctions that drive the current framework.

Thus, even with a coherent response to the problems addressed above, there is every reason to expect that new problems would emerge rapidly, leaving the regulatory coverage again uncertain. The basic point is that such problems are inevitable until and unless a more functional code is adopted to govern electronic payments generally. Meanwhile, the minor change discussed above[92] could at least make the system as coherent for these transactions as it is for conventional transactions.

IV. ENSURING REGULATORY COMPLIANCE

Part III of this paper operates entirely within the framework of the existing regulatory apparatus. Thus, it is limited to considering the extent to which GLB and the EFTA/E and TILA/Z regimes replicate for the new transactions the regulatory environment that they impose on conventional transactions. This Part examines the

---

[89] *See* Cooter & Rubin, *supra* note 62, at 89 (making that point generally).

[90] See *supra* notes 80-82 and accompanying text.

[91] *See* sources cited *supra* note 11.

[92] *See supra* note 83.

regulatory system from a broader perspective. It starts by focusing on a fundamental problem implicit in the existing system: the distinction between the level of responsibility to be expected from conventional financial institutions and that to be expected from the new Internet-based intermediaries. It then discusses three types of potential regulatory approaches. Finally, it summarizes tentative recommendations for the P2P and EBPP contexts based on what we currently know about them.

A. The Problem

The EFTA and TILA use the typical apparatus of the modern federal regulatory statute: provisions for class actions, statutory damages, attorney fees, and the like.[93] Accordingly, it would be natural to conclude that a careful analysis of the problems discussed in Part III of this paper should be enough to resolve the problem. Once the EFTA/E and TILA/Z regimes are brought up to date, we might think, the new entities would comply and all would be well.

Two general concerns, however, make that optimistic outlook seem implausible. First, it is doubtful that the kinds of civil-liability regimes at hand – which rely primarily on litigation by small and dispersed consumers – will be able to control the behavior of the large businesses at which they are directed. That is particularly true in this context, where the facts of each unauthorized transaction and billing error often will be specific to each individual consumer.[94]

Second, the pervasive federal regulation of banks substantially increases the likelihood that banks will comply with their obligations under the TILA/Z and EFTA/E regimes. At the most basic level, the direct purpose of much of federal banking regulation – federal supervision of capital maintenance and lending practices – is to ensure the solvency and fiscal prudence of the institutions.[95] If that regulation is even marginally effective,[96] it increases the likelihood that banks will have the assets necessary to comply with their obligations under those statutes. That might seem like a small thing,

---

[93] EFTA § 915; TILA § 130.

[94] *See, e.g.*, Cooter & Rubin, *supra* note 62, at 80-82 (discussing difficulties consumers face in suing financial institutions).

[95] *See, e.g.*, Alvin C. Harrell, *Deposit Insurance Issues and the Implications for the Structure of the American Financial System*, 18 OKLA. CITY U. L. REV. 179, 179 (1993).

[96] For general economic analysis of the effects of the American system on the incentives of institutions and their customers, see Jonathan R. Macey & Geoffrey P. Miller, *Bank Failures, Risk Monitoring, and the Market for Bank Control*, 88 COLUM. L. REV. 1153, 1200-01 (1988); Robert C. Merton, *An Analytic Derivation of the Cost of Deposit Insurance Loan Guarantees*, 1 J, BANKING & FIN. 3 (1977); Kenneth E. Scott, *Deposit Insurance and Bank Regulation: The Policy Choices*, 44. BUS. LAWY. 907 (1989). There is of course considerable doubt about how to design an optimal banking regulatory system. For insightful discussions of other systems, see Curtis J. Milhaupt, *Japan's Experience with Deposit Insurance and Failing Banks: Implications for Financial Regulatory Design*, 77 WASH. U.L.Q. 399 (1999); Geoffrey P. Miller, *Deposit Insurance Inevitable? Lessons from Argentina*, 16 INT'L REV. L. & ECON. 211 (1996).

but the likelihood that a major Internet payment fraud could create a regulatory responsibility beyond the assets of a small dotcom P2P provider is plausible.[97] That is particularly true given the likelihood that those providers will be targets for fraudulent activity, as PayPal has been.[98] More generally, the persistent supervision and need to accommodate regulators on a regular basis makes it quite difficult for a bank to adopt a cavalier attitude about regulatory compliance.[99]

The same analysis applies to privacy obligations. It does not take a hardened cynic to think that the chances of systematic noncompliance – or even lackadaisical compliance that tolerates a significant number of low-level violations – is much more likely for unregulated companies than for regulated depository institutions.[100] In assessing that likelihood, it is important to note that GLB, unlike TILA and the EFTA, does not provide for a private cause of action.[101] Finally, it also is worth wondering whether smaller companies that are unregulated and financially constrained will be adequately motivated to expend the resources necessary to protect their consumer's information from unauthorized access by third parties.

To put the point generally, the regulatory regimes directed to the activities of the new payment intermediaries depend in part for their effectiveness on the background regulatory supervision of the banks governed by those regimes. Because nonbank payment intermediaries are not generally subject to that supervision,[102] there is a cognizable risk that they will show less care in complying with those regimes than

---

[97] *See* Kuttner & McAndrews, *supra* note 11, at 41-42 (noting the liquidity risk that would arise if payment intermediaries handled larger numbers of transactions and the regulations that limit that risk for banks); Spiotto & Mantel, *supra* note 11, at 20 (noting "the rapid emergence in the past two years [before 2001] of small aggregators with few assets").

[98] *See* Gilbert, *supra* note 79; Christopher Null, *Bogus Alerts Target PayPal Users*, WIRED NEWS, Feb. 14, 2003, *at* http://www.wired.com/news/ebiz/0,1272,57673,00.html (last visited Mar. 13, 2003) (discussing schemes that sent PayPal users to bogus sites at www.paypai.com and www.paypalsys.com); Rosencrance, *supra* note 9.

[99] Consider the pervasive preoccupation with a bank's Community Reinvestment Act obligations of regulators examining wholly unrelated transactions. *E.g.*, Kenneth H. Thomas, *CRA at 25: Reforming an Almost Perfect Law*, AM. BANKER, Dec. 13, 2002, at 6, *available at* 2002 WL 26548785. The parallel is not perfect, of course, because the CRA is specifically designed to lead to the conditioning of merger transactions on a good record of CRA compliance, *see, e.g.*, *id.*, but the point still seems valid. The pervasive control of banking regulators makes it seem most difficult for a bank consciously to maintain a pattern of regulatory noncompliance.

[100] *See* Radecki & Wenninger, *supra* note 35, at 5 (noting that concern).

[101] *See* 15 U.S.C. § 6805 (authorizing enforcement by regulatory authorities); MANN & WINN, *supra* note 2, at 159.

[102] *See supra* page 2.

conventional depository institutions.[103] The next section discusses three types of potential responses to that problem.

B. Potential Responses

Because of the fluid and rapid pace of development in the industry, it is difficult to design a response to the regulatory gap discussed in the previous section. Accordingly, I start in this section with a general analysis of the pros and cons of three general approaches: doing nothing, adopting more onerous regulation of Internet payment intermediaries, or imposing liability on banks for the failure of the intermediaries to comply with their regulatory obligations. The paper concludes in the next section with an application of that analysis that includes tentative recommendations on the best course of action under current circumstances.

1. Doing Nothing

The first possibility is to do nothing. At this point, the concerns expressed above are largely (though not entirely[104]) conjectural. An advantage of the current system is that it permits ready entry into the market, which has facilitated rapid development of the competing business models and vigorous competition among the various providers. Thus, the P2P market is growing rapidly and already has experienced a considerable shakeout of weaker and unsuccessful providers.[105] The EBPP market is even more fluid, so it is too soon even to predict exactly what types of services ultimately will be provided.[106] Any regulatory intervention almost inevitably would heighten barriers to entry in the industry. That, in turn, would be likely to have the immediate effect of limiting competition, particularly by smaller and newer companies.[107] Thus, that approach might drive intermediaries from the market, even if their model ultimately might have become prevalent in the marketplace.[108]

---

[103] *See* Kuttner & McAndrews, *supra* note 11, at 42 (noting that protecting customers against fraudulent use of their accounts "is a major concern"); Mester, *supra* note 11, at 16 ("[T]hey still deserve monitoring. For example, they may expose individuals and institutions using them to substantial liability through fraud.").

[104] *See infra* notes 143 (noting existing complaints about P2P providers) & 149 (noting existing complaints about EBPP providers).

[105] *See supra* notes 15-17 and accompanying text.

[106] *See, e.g.*, Andreeff et al., *supra* note 9, at 5-10 (detailed discussion of various competitors evincing an inability to predict which, if any, of the existing models will succeed in the market).

[107] I assume a considerable economy of scale and learning curve in enduring regulatory burdens.

[108] *See* Andreeff et al., *supra* note 9, at 9 (expressing that view).

In assessing the weight of that concern, it is important to credit the importance of "network" or "bandwagon" effects[109] in this industry.[110] Thus, PayPal's success in the P2P market shows some of the signs of a successful implementation of a lock-in strategy: an early effort to acquire customers by offering services at a very low (indeed, negative) price, which led to rapid growth of a customer base, and was followed in turn by the imposition of substantial transaction fees.[111] Without that kind of sustained effort, it is very difficult for that kind of network good to obtain a sufficient critical mass of users to reach the maximum optimal level of deployment. It would be unfortunate if a well-intentioned regulatory intervention had the effect of stifling the competition necessary for such products to be introduced successfully. Of course, on the other hand, the absence of regulatory intervention may enhance the possibility that the competition will go beyond robust to unfair. That concern seems less significant, however, given the fact that the existing players – the ones who would be at risk of harm from unduly aggressive competition – are financial institutions (presumably capable of protecting themselves from such conduct).

2. Direct Regulation of Intermediaries

The second possibility is to adopt some form of regulatory supervision for Internet intermediaries. The benefits of that approach are obvious. First, it enhances protections for consumers by providing a backstop to the direct legal obligations of intermediaries, parallel to the backstop that federal regulatory authorities provide for banks. Second, it levels the playing field left uneven in the present arrangement, in which banks always are subject to intensive regulatory supervision but Internet payment intermediaries are subject to lesser supervision (or none at all).

---

[109] For general discussion of how those effects can "lock in" an early industry leader's success, see ROHLFS, *supra* note 46, chs. 3-4; CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES ch. 5 (1999). As Rohlfs explains, the basic idea is that some products have external demand-side scale economies – features external to the production process that make demand for products increase as the number of units of the product already sold increases. *See* ROHLFS, *supra* note 46, at 55. For a well-reasoned skeptical view about the common occurrence of lock-in, see STAN J. LIEBOWITZ & STEPHEN E. MARGOLIS, WINNERS, LOSERS & MICROSOFT (1999) (collecting and amplifying a substantial body of periodical literature by Liebowitz and Margolis).

[110] *See* Kille, *supra* note 35, at 3 (noting that "sufficient use by recipients" is the "KEY requirement for successful" use of electronic presentation of bills); James J. McAndrews, *Network Issues and Payment Systems* 22-24, BUS. REV. (Fed. Res. Bank of Phila.), NOV./DEC. 1997, at 15, 22-24 (noting a number of examples in the payments context, including ATM adoption and PIN-based debit cards); Mester, *supra* note 11, at 14-15; Radecki & Wenninger, *supra* note 35, at 5.

[111] *See* Leuty, *supra* note 22 (discussing the development of PayPal's fee and revenue structure); SHAPIRO & VARIAN, *supra* note 109, ch. 6 (frank discussion of how to execute a successful lock-in strategy). In economic terms, the problem is to obtain a sufficiently large critical mass of users to allow expansion of the market to the maximum equilibrium user set. *See* ROHLFS, *supra* note 46, at 20-28. For case studies on successful – and unsuccessful – attempts to obtain that critical mass, see ROHLFS, *supra* note 46, ch. 6-13.

The first issue is to decide what type of regulatory system would be appropriate. Because the entities are not themselves holding demand-deposit accounts, the case for full-scale bank regulation is quite weak. Among other things, they are not subject to the kinds of "runs" that make the stability of depository institutions an important object of public policy.

Accordingly, the appropriate form of regulation would be something less intrusive, similar to the existing regulation of money transmitters (to which PayPal is subject in many states).[112] That regulation generally requires businesses to obtain a state license,[113] imposes periodic reporting requirements,[114] and makes them subject to audits by state officials.[115] It also often includes minimum net worth[116] or bond requirements[117] or imposes restrictions on permissible investments.[118]

The next issue is to decide at what level the regulations should be imposed. Money transmitters currently are regulated at the state level, not the federal level.[119] As that industry has become more consolidated, considerable pressure has arisen for more uniformity in the various state regulatory schemes. That pressure, in turn has led to the recent drafting and promulgation of the proposed Uniform Money Services Act (already adopted in Iowa, Vermont, and Washington).[120] Although that statute probably would not apply to EBPP providers in its current form, its substantive provisions provide a useful and up-to-date template for regulation.

The difficult question, however, is whether state – rather than federal – regulation is appropriate. Concerns about inconsistent state regulations weigh even more heavily

---

[112] *See State Licenses*, *available at* http://www.paypal.com/cgi-bin/webscr?cmd=p/ir/licenses-outside (last visited Apr. 29, 2003).

[113] *See, e.g.*, ARIZ. REV. STAT. § 6-1202; § 205 ILL. CONS. STAT. 657/10; MINN STAT. § 53B.02; TEX. FIN. CODE § 152.201; VA. CODE § 6.1-371.

[114] *See, e.g.*, ARIZ. REV. STAT. § 6-1211.

[115] *See, e.g.*, § 205 ILL. CONS. STAT. 657/55.

[116] *See, e.g.*, N.J. STAT. § 17:15C-5; TEX. FIN. CODE § 152.203.

[117] *See, e.g.*, ARIZ. REV. STAT. §§ 6-1205.01; § 205 ILL. CONS. STAT. 657/30

[118] *See,e.g* .,A RIZ. REV. STAT. § 6-1212; § 205 ILL. CONS. STAT. 657/50; MINN STAT. §§ 53B.06, 53B.08.

[119] However, the operation of an unlicensed money transmitter business is a federal criminal offense. 18 U.S.C. § 1960.

[120] The text of the final version of the Act (promulgated in 2001) is available at http://www.law.upenn.edu/bll/ulc/moneyserv/UMSA2001Final.htm (last visited Mar. 13, 2003) [hereinafter cited as UMSA]. For discussion, see Taft, *supra* note 52, at 43-44. For enactment updates, see Legislative Activity by Act (2002-2003) at http://www.nccusl.org/nccusl/LegByAct.pdf (last visited Sep. 14, 2003) (shows enactment in Iowa and Washington).

for Internet-based businesses than they do for brick-and-mortar businesses.[121] That is particularly true as the share of cross-border payments increases – which raises the prospect of regulation not only by the several states of this country, but also by foreign countries as well.[122] Thus, although the simplest path for the time being might be to foster broad enactment of something like the Uniform Money Services Act (broadened to cover EBPP providers), it is difficult to believe that anybody trying to design a rational system would conclude that parallel regulation by all local jurisdictions is the most appropriate way to regulate the Internet-based entities under discussion.

A second possibility would be to allow regulation of the intermediary in a particular state jurisdiction in which the intermediary could be said to be located.[123] Internet scholars have tried hard to resolve such choice-of-law questions to make a territorial allocation of regulatory authority.[124] To the extent those efforts speak to this question, they generally suggest that each jurisdiction in which the consumers reside would have the *power*to regulate the entities in question. [125] There is not, however, any clear consensus about a basis for a particular location taking the regulatory lead, largely

---

[121] The irrationality of subjecting Internet-based businesses to widely varying state regulatory schemes has been the principal reason that Congress persistently has protected those entities from state sales and use taxes. *See* Internet Tax Freedom Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998) (imposing a three-year moratorium on a variety of Internet related taxes); Internet Tax Nondiscrimination Act, Pub. L. No. 107-75, 115 Stat. 703 (2001) (extending the moratorium to November 1, 2003). The recent willingness of states to harmonize their sales-tax systems – spurred by their serious needs for new revenues – well may convince Congress to remove the bar on such taxation. *See* Brian Krebs, *Study Questions Net Tax Payoff* (Mar. 13, 2003) *at* http://www.washingtonpost.com/wp-dyn/articles/A21580-2003Mar13.html (last visited Mar. 13, 2003). Thus, if the States could coalesce around something like the UMSA, the costs of state regulation might diminish considerably.

[122] The problem is potentially even more complicated, if the use of P2P providers to send international transfers becomes a significant market. Currently, that market is dominated by depositary institutions like CitiBank. *See supra* note 17 (discussing international P2P transfers). PayPal, however, is beginning to play a significant part in that market as well, and has experienced some widely noted difficulties. *See* Drew Cullen, *How Many Brits Were Robbed Today?*, THE REGISTER (U.K.) (Feb. 27, 2003), *at* http://www.theregister.co.uk/content/6/29508.html (last visited Mar. 17, 2003) (describing errors caused by an incorrect dollar-pound exchange rate at the PayPal site); Drew Cullen, *PayPal Reimburses Brits*, THE REGISTER (U.K.) (Mar. 1, 2003), *at* http://www.theregister.co.uk/content/6/29532.html (last visited Mar. 17, 2003) (describing plans to reimburse customers).

[123] *See, e.g.*, UCC § 9-307(e) (adopting a bright-line rule for purposes of personal-property lending that a corporation is located in the jurisdiction under whose laws it is organized).

[124] *E.g.*, American Bar Association Global Cyberspace Jurisdiction Project, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*, 55 BUS. LAWY. 1801 (2000) [hereinafter *ABA Cyberspace Jurisdiction Project*].

[125] *See ABA Cyberspace Jurisdiction Project*, *supra* note 124, at 1905-15 (discussing jurisdictional issues for payment systems and banking services provided over the Internet).

because there is a clear consensus that the location of the physical aspects of the system (the Web server that contains the Web site, for example) should not be dispositive.[126]

Moreover, even if a consensus could be reached – under which all of the States (and affected foreign countries) – would agree that a single State would have the sole power to regulate the entity, a substantial problem would remain in the gross lack of symmetry between the reach of the regulated market (basically national, with international aspects) and the constituency of the regulator (statewide). Relying on basic public choice concepts, that lack of symmetry imposes a substantial risk that the jurisdiction in which the intermediary is located will adopt rules unduly favorable to the intermediary. That risk is particularly salient if the jurisdiction obtains substantial benefits from the location of the intermediary in the jurisdiction (through employment or taxes, for example), while most of the intermediary's customers are located in other jurisdictions.[127]

The basic problem is that the issues that motivate the regulation are not sufficiently related to state-level variations and circumstances to make state-level regulation optimal. Thus, it seems clear that the best approach would be a federal statute. That is not to say, of course, that state law-enforcement authorities are not so interested in the closely related problem of money laundering that they will resist any lessening of their authority in the area. It is to say, however, that these issues of consumer protection are more likely to be addressed optimally at the federal level.

At the federal level, the simplest response would be to require these services to be provided by banks, which would obviate the need for any specific regulatory legislation. As discussed above, however, the business that these intermediaries operate suggests that bank-type regulation is unduly onerous. Thus, a better approach would be regulatory legislation tailored for these intermediaries. It might seem implausible in the current environment to expect Congress to create a new federal regulatory regime.[128] That is

---

[126] *See ABA Cyberspace Jurisdiction Project*, *supra* note 124, at 1908-11.

[127] This is, of course, an argument parallel to the race-to-the-bottom discussion in corporate law. Whatever the truth of the matter on that issue, the problem seems more serious here because of the lack of symmetry discussed in the text.

[128] The poor response to Federal Reserve efforts to consider the appropriate level of regulation for stored-value cards is the most obvious example. The story starts with the Federal Reserve's proposal of some mild regulations. *Proposed Rules, Federal Reserve System*, 59 FED. REG. 10684 (1994). Hostile reaction led the Federal Reserve to change the regulatory proposal into a report to Congress. Board of Governors of the Federal Reserve System, *Report to the Congress on the Application of the Electronic Fund Transfer Act to Stored-Value Products* (March 1997) *at* http://www.federalreserve.gov/boarddocs/rptcongress/efta_rpt.pdf (last visited Mar. 13, 2003). Adverse reaction to that report led the Federal Reserve to effectively table it: no action has been taken in the six years since the report was sent to Congress. *See* Taft, *supra* note 52, at 45 (suggesting that the Fed did not pursue the proposal because "concerns about hindering the development of new technology prevailed over additional protections for consumers using stored-value products"). This is of course an obvious change from previous decades, when it was plausible to think that Congress would step in to protect consumers when neither the UCC nor the

particularly true when the regime seems to fall in the area of commercial law that Congress traditionally has left to state regulation. On the other hand, the recent experience of the Check 21 Act (passed by both houses of Congress during its current legislative session)[129] suggests that the Board of Governors of the Federal Reserve enjoys a sufficiently influential position with Congress to obtain enactment of legislation designed to ensure the effective operation of the payment system. Given the interest (noted above) that researchers at the Federal Reserve's constituent banks have taken in these developments, it does not seem far-fetched to think that the Federal Reserve might take the lead in developing such a statute.

3. Regulating Banks as Gatekeepers

The final approach is the most adventurous: directly obligating banks to ensure compliance with the EFTA/E and TILA/Z regimes for all transactions at the bank. The premise here is to view the bank as a gatekeeper that will both monitor the intermediary to ensure that it behaves appropriately and exclude those that cannot be induced to behave appropriately.[130]

Because the problems discussed in Part III arise only if the intermediaries can access accounts at the bank, the bank (at least theoretically) is in a position to control the activities of the intermediaries. For example, the simplest response to such a scheme might be for the bank to provide by contract that the intermediary would be responsible to the bank for the costs that the bank incurs for Regulation E compliance related to

---

Federal Reserve would take action. *See* Robert D. Cooter & Edward L. Rubin, *Orders and Incentives as Regulatory Methods: The Expedited Funds Availability Act of 1987*, 35 UCLA L. REV. 1115, 1130-50 (1988). Indeed, the hostility to *any* new regulation poses a substantial obstacle to the suggestions that I make in Part III, *supra* note 83 and accompanying text.

[129] The House on June 5 passed the Check 21 Act, H.R. 1474. The Senate on June 26 passed its version, the Check Truncation Act, S. 1334. The statute generally is designed to facilitate the processing of checks by means of images instead of the cumbersome paper originals. For explanation from the Federal Reserve (which drafted the statute), visit http://www.federalreserve.gov/paymentsystems/truncation/default.htm. The same topic was within the mandate of the Drafting Committee recently charged with promulgating revisions to UCC Articles 3 and 4 (of which I was the Reporter). The Committee was unable to pursue that topic because of its inability to produce a consensus regarding an appropriate reconciliation of the interest in technological advance with the concerns of consumers about continuing to receive their cancelled checks. The Federal Reserve, of course, is free to proceed at the federal level without such a consensus.

[130] For the most general formulation of this regulatory structure, see Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986) [hereinafter Kraakman, *Gatekeeper Anatomy*]. Within Kraakman's framework, this would be an instance of the use of gatekeeper liability to remedy enforcement insufficiency. For a general discussion, see Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857, 888-96 (1984) [hereinafter Kraakman, *Corporate Liability Strategies*].

transactions that the intermediary conducted on the accounts of the bank's customers. It would be up to the bank to take cost-effective steps to minimize the costs that the bank incurs from any failure of the intermediary to satisfy those obligations: it might require the intermediary to obtain a letter of credit from another institution, post a bond, or simply deposit a reserve of funds in the bank against which the bank could draw for those expenses.

That approach has several benefits. One obvious benefit is that it protects consumers from asset insufficiency on the part of the intermediaries.[131] The gatekeeper strategy is uniquely suited to situations in which practicable legal remedies are not adequate to ensure full compliance with regulatory responsibilities.[132] Another potential benefit of that approach relates to the likelihood that the banks on which the risk of loss ultimately would fall are larger, better capitalized, and more diversified in the range of their operations than the intermediaries for whom the banks are to be the gatekeepers. Specifically, if the greater size and financial sophistication of the banks makes it more cost-effective for them to bear and spread those losses, then the gatekeeper regime would lower the total cost of those losses.[133]

A more general benefit is that the bank should be more effective at monitoring the activities of the provider than government regulators. That would be true because the bank arguably[134] would have a strong incentive – maximizing the value of the account services received by its customers – to ensure that the regulations that it imposes on the intermediaries do not unduly burden the activities of the intermediaries. If the bank attempts to exclude those intermediaries by imposing excessive burdens on them – burdens that are not cost-justified – the bank would reduce the net value of the services that the bank could extract from its customers. If so, we might expect that customers would migrate to banks that reach more effective arrangements with the intermediaries.

The banks should be in a better position than any government regulator to assess in a dynamic and informed way the relative benefits and burdens of various responses that the bank might take in response to a gatekeeping responsibility.[135] For example, the banks are likely to assess the legitimacy of the activities of the intermediary much more

---

[131] *See* Kraakman, *Corporate Liability Strategies*, *supra* note 130, at 869-71 (discussing that potential benefit of gatekeeper strategies).

[132] Kraakman, *Gatekeeper Anatomy*, *supra* note 130, at 56.

[133] *See* Kraakman, *Corporate Liability Strategies*, *supra* note 130, at 864-67.

[134] This discussion assumes, of course, that the bank is not motivated by anti-competitive concerns to stifle the intermediary's service. I discuss that problem *infra* notes 141-142 and accompanying text.

[135] In Kraakman's terms, this is a "chaperone" regime, in which "gatekeepers can detect and disrupt misconduct in an unfolding relationship" with enforcement targets. Kraakman, *Gatekeeper Anatomy*, *supra* note 130, at 63.

knowledgeably than any regulator could.[136] In addition, given the circumstances, it seems unlikely that the banks would cooperate with the intermediaries in misconduct – a particularly topical concern in gatekeeping arrangements in a post-Enron environment.[137]

In sum, the bank would be in a position to make intelligent, market-driven choices about how to trade off expenditures on monitoring the activities of the intermediary versus simple reliance on monetary assurances from the intermediary or bonds from fiscally responsible third parties. That is particularly important given the complicated, technology-sensitive, and rapidly developing nature of the industry.

There are of course several obvious problems with the gatekeeper approach. First, it would be likely to increase the costs of the bank's activities, and thus the costs of the services provided to the bank's customers. In an era when the number of consumers who are priced out of the market for banking services already is sufficiently high to be a cause for policy concern, any initiative that might aggravate that problem warrants serious scrutiny. The twin premises of this approach, however, would be (1) that those costs would not be substantial unless there was a substantial risk that the intermediaries would fail to comply if left to their own devices (thus letting those costs fall on consumers in any event); and (2) that the banks are much better situated than government agents to identify and minimize those costs.

Another problem with this approach is that it does not address privacy issues at all. Because a simple monetary remedy does not as easily remedy privacy issues – restoring funds improperly removed from the consumer's deposit account – this type of remedy offers no protection on that score.

Another obvious problem is technological: the effectiveness of the approach depends entirely on the ability of banks in fact to control the conduct of the intermediaries.[138] As the controversy over screen-scraping suggests, it is not clear that current technology permits banks to prevent intermediaries from accessing their customers' accounts without their consent. The reason is that it is difficult for the bank to

---

[136] *See* Stephen Choi, *Market Lessons for Gatekeepers*, 92 NW. U. L. REV. 916, 925-27 (1998) (emphasizing the importance of "screening accuracy" to a successful gatekeeper strategy); Kraakman, *Corporate Liability Strategies*, *supra* note 130, at 891 (emphasizing the importance to successful gatekeeper strategies of "low-cost access to information about firm delicts"). Assaf Hamdani amplifies this point in great detail in his as-yet unpublished working paper. Assaf Hamdani, *Assessing Gatekeeper Liability* (unpublished draft on file with author).

[137] *See* John C. Coffee, Jr., *Understanding Enron: It's About the Gatekeepers, Stupid*, 57 BUS. LAWY. 1403 (2002); Kraakman, *Gatekeeper Anatomy*, *supra* note 130, at 69-72 (emphasizing the importance of avoiding "corruption" of gatekeepers); Kraakman, *Corporate Liability Strategies*, *supra* note 130, at 891 (emphasizing the importance of using "incorruptible outsiders" as gatekeepers).

[138] *See* Hamdani, *supra* note 136; Kraakman, *Gatekeeper Anatomy*, *supra* note 130; Kraakman, *Corporate Liability Strategies*, *supra* note 130, at 890 ("The first requisite for gatekeeper liability is, of course, an outsider who can influence [the subject] to forgo offenses.").

distinguish between two different persons accessing the Web site. If both the intermediary and the customer have the customer's userid and password, the bank's server probably will not be able to ascertain which of the two is accessing the account on any particular occasion.[139] If that is true, then technology alone will not permit the bank to use the threat of exclusion to control the intermediary's access.

That technological problem, however, seems unlikely to be a serious problem of regulatory design. It would be easy enough to impose a general prohibition (akin to the Consumer Fraud and Abuse Act, 18 U.S.C. § 1030 (the CFAA)) on accessing a customer's account without the consent of the bank.[140] With a broadening of the CFAA, intermediaries would not be able to access deposit accounts without permission from the bank. The bank, in turn, could condition its permission on the formation of a contract relationship with the intermediary that would include whatever terms were appropriate to implement the bank's responsibility for regulatory compliance.

Finally, the most serious difficulty with that approach is the possibility that it will have a markedly adverse competitive effect. As the discussion above emphasizes, both the P2P and EBPP markets currently include a number of nonbank entities competing directly against banks.[141] A regime in which banks control access to the accounts for which payment intermediaries provide services may not be as exclusive as a regime in which those services can be provided only by banks, but the potential for anti-competitive conduct is obvious. If applicable regulations permit banks to impose onerous terms on the intermediaries, then the bank's ability to drive those providers from the marketplace might be enhanced.[142]

---

[139] The controversy over the use of screen-scraping for financial institutions to collect comprehensive profiles of their customer's financial affairs strongly suggests this problem, because that controversy rests on the premise that the "screen-scraper" can scrape information from another bank's Web site without the knowledge of the bank operating the site. *E.g.*, Andreeff et al., *supra* note 9, at 9; Andrew Roth, *CheckFree Says It Will Use Screen Scraping*, AM. BANKER, Mar. 22, 2001, at 10 (describing screen scraping as "a practice by which information is simply lifted from a Web site, generally without the site owner's permission or knowledge").

[140] Screen scraping and EBPP services generally do not violate that statute because the screen scrapers and EBPP providers have authorization from the customer. *But cf. infra* note 149 (discussing settled litigation in which First Union Bank claimed that PayTrust's procedures violated the Computer Fraud Abuse Act).

[141] *E.g.*, Chandler, *supra* note 35, at 2 (noting the competition between banks and newer entrants over the new "delivery channels"); Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. 675 (1999) (noting the rise of new payments entities to compete with the existing businesses).

[142] The hostility of banks to intermediary access to their accounts is not purely hypothetical. For example, see the litigation between First Union and PayTrust mentioned *infra* note 149.

On the other hand, that kind of conduct would be effective only if banks as a group colluded to exclude the intermediaries. As discussed above, a bank that tried to impose undue burdens on intermediaries to exclude them from the bank's customers would face competition from other banks that might try to maximize the value of services they could provide to their own customers by entering into value-increasing arrangements with intermediaries. Because the banking industry is highly competitive, there is some reason to doubt that collusive exclusionary tactics would be effective. Moreover, particularly in light of the competitive structure of the banking industry, it may be reasonable to rely on traditional antitrust enforcement to protect providers from such practices.

C. Recommendations

For several reasons, it is not plausible at this stage to offer a definitive "answer" to the problem of regulatory strategy that this paper addresses. For one thing, the industries are developing and changing so rapidly that the object of inquiry is a moving target. For another, there is so little information about how the systems in fact operate that it is difficult to assess the weight of the competing concerns: we know next to nothing about the rates of fraud and error in these systems, about the culture of data privacy in the industry, and about the degree of compliance with regulatory responsibilities. Finally, because the possible risks of allowing unregulated access to consumer deposit accounts and of hasty intervention in a fluid competitive situation are not readily balanced against each other, an element of frank judgment is necessary to resolve a conflict between them.

Still, the analysis of the alternatives presented above does support some tentative recommendations about the most promising avenues of relief. The recommendations that follow take the perspective that the correct answer to the problem is to provide consumers protections as close to what they have for conventional financial relationships as seems practicable, without unduly harming the potential for competition and innovation in the industry. Those recommendations reflect in part an attempt to foster outcomes likely to be consistent with consumer expectations. The recommendations also reflect an implicit willingness to place considerable weight on concerns about privacy issues. It seems much more troubling from a privacy perspective to have consumer financial information in the hands of wholly unregulated and thinly capitalized companies than in the hands of banks. In any event, because the recommendations rest heavily on those perspectives, it is worth emphasizing that policymakers who do not weigh those concerns so heavily would reach different conclusions.

1. P2P Intermediaries

Selecting a regulatory approach for the P2P intermediaries is difficult for a variety of reasons. First, because of the persistent allegations of misconduct by PayPal – none of which, to be sure, seem to have resulted in any *proof* of serious misconduct – it seems

unacceptable to have PayPal completely unregulated.[143] At the same time, the competitive landscape shows a tension between PayPal – now owned by eBay – and smaller competitors primarily controlled by banks. In that setting, it seems particularly inappropriate to use the gatekeeper strategy to subject PayPal's operations to the control of the banking industry. For the same reason, it seems absurd to say that P2P services must be provided by a bank. That is simply to require eBay to sell PayPal to a bank. The evident synergy between PayPal's operations and eBay's suggests that any such outcome would unnecessarily destroy some significant opportunity for innovation in the provision of payment services.[144]

My views on that point are strongly influenced by the potential of PayPal to be a major competitive figure as Internet payment systems develop in the years to come. For example, it is a well-known aspect of the Internet that the payment systems available for Internet retailers are wholly inadequate: they are both expensive and subject to high rates of fraud (the costs of which are born directly by the retailers).[145] Yet, the major credit-card networks have retained a dominant near-monopoly position in that market.[146] PayPal is already one of their strongest competitors, as it provides payment services to smaller merchants that find it uneconomical to join Visa or MasterCard directly.[147] It may be that an unconstrained PayPal has the potential to be a risk for consumers.

---

[143] I have no basis for forming an opinion about the merits of those allegations. I simply note that they are quite numerous. For eBay's formal disclosure about litigation related to those problems, see eBay Inc., Form 10-Q, at 15 (Sept. 30, 2002) *available at* http://www.sec.gov/Archives/edgar/data/1065088/000089161802005206/f85887e10vq.htm#011 (last visited Mar. 17, 2003). For news stories about those problems, see, *e.g.*, Craig Bicknell, *Anti-Fraud That's Anti-Consumer*, WIRED NEWS, July 24, 2000, *at* http://www.wired.com/news/business/0,1367,37642,00.html (last visited Mar. 13, 2003) (discussing frustration of customer whose credit card was deemed suspicious by PayPal anti-fraud program); Dan Knight, *PayPal Insecurity* (Aug. 8, 2002) *at* http://lowendmac.com/musings/02/0808.html (last visited Mar. 13, 2003); Keith Regan, *PayPal Users Sue over Frozen Funds* (Mar. 13, 2002), *at* http://www.ecommercetimes.com/perl/story/16751.html (last visited Mar. 13, 2003) (lawsuit alleging failure to comply with Regulation E). For a few of the sites collecting criticism of PayPal, see http://www.paypalwarning.com/ (last visited Mar. 13, 2003); http://www.paypalsucks.com/ (last visited Mar. 13, 2003); http://www.killpaypal.com/ (last visited Mar. 13, 2003).

[144] *See, e.g.*, Peter Lucas, *eBay Puts Its Mark on PayPal*, CREDIT CARD MANAGEMENT, April 2003, at 34 (discussing eBay's strategic use of its control of PayPal).

[145] *See ePaynews Online Fraud Data*, *supra* note 1. The basic Visa electronic commerce interchange rate, for example, is 1.80% plus $.10. That is considerably higher than the base (CPS Retail) rate of 1.37% plus $.10. *Visa Interchange Compliance*, http://www.cardweb.com/carddata/charts/MerchantFees/2002/visa.doc (last visited Apr. 29, 2003).

[146] *See supra* note 1.

[147] *See* Mantel & McHugh, *supra* note 5, at 5-6 (noting the potential for P2P providers to provide competition in the provision of payment services to small businesses).

However, at the same time an unconstrained PayPal that forces Visa, MasterCard, and the banking industry to look constantly over their shoulders could do more for the competitiveness of Internet payment providers than any pressure that the Antitrust Division of the Department of Justice has brought to bear.[148]

More broadly, the introduction of this paper notes the persistent failure of electronic-money products to take hold on the Internet. If there is a market for a new and innovative electronic-money product, the likelihood that such a product will be developed, implemented, and deployed successfully is maximized by a regulatory system that permits the continuing presence of a large player like PayPal not wedded to the existing payments networks.

The foregoing comments seem to leave a choice between doing nothing and adopting the light federal regulatory regime discussed above. Doing nothing of course does not leave PayPal completely unregulated, because it already is under the supervision of money-transmitter statutes in a number of states. And the events to date make it difficult to be sure that the risk of duplicative or inappropriate regulation – either excessive or too lenient – will cause problems. In any event, in a perfect world, a single federal arrangement would make more sense. Given the fact that PayPal's parent eBay already must comply with the increasingly onerous requirements that come with its listing on NASDAQ, it seems unlikely that those requirements would impose costs that would have competitive significance to PayPal. And at the same time they should go far to assuage the concerns summarized above about PayPal's responsibility for its regulatory obligations.

2. EBPP Intermediaries

It is much harder to come to rest on a recommendation for the EBPP systems. The nature of their operations makes the privacy and fraud concerns much more substantial than in the P2P context – because their operations necessarily involve pervasive access to consumer deposit accounts. P2P providers by contrast, are likely for many consumers to conduct their operations without any mechanism for accessing the consumer's deposit account. To be sure, there are few reports of problems with the EBPP systems to date.[149] But the fluidity of the highly fractionated market gives little

---

[148] The government recently obtained a trial-court judgment against Visa and MasterCard in an antitrust action challenging several aspects of the industry's structure. *U.S. v. Visa, Inc.*, 2002 WL 638537 (S.D.N.Y.).

[149] PayTrust has generally gotten good marks on such questions. *See, e.g.*, Don Willmott, *Bill Payment* (Nov. 28, 2000) *at* http://www.zdnet.com/products/stories/reviews/0,4161,2658209,00.html (last visited Mar. 13, 2003) (lauding insurance for negligent and fraudulent transactions); *PayTrust: On Being Trustworthy to Pay the Bills at* http://www.theexaminer.biz/Security/paytrust.htm (last visited Mar. 13, 2003) (lauding PayTrust security efforts). On the other hand, one Federal Reserve analyst has noted a conspicuous lack of common error-resolution services by EBPP providers. *See* Mantel, *supra* note 2, at 26-27.

basis for confidence that all members of the industry will be responsible. Thus, it seems unacceptable to think that the current regulatory framework will be suitable in the end.

At the same time, it seems excessive to say that only banks can provide those services. Among other things, a rule limiting those services to banks would significantly diminish the likelihood of a universal payment service. In the end, there seems to be a strong case that such a site is at least part of the optimal response, because it would be easier for such a site to overcome the classic bandwagon-effects problems of attracting sufficient billers and consumer payers as customers.[150] Of course,such a site still could develop in a "bank-only" approach – for example through contracts by individual banks with a dominant provider like CheckFree. But to the extent that a bank-only approach lessens the potential for such a service, it is a serious cost of the approach.

That leaves for consideration the intermediate approaches of industry-specific regulation and the use of banks as gatekeepers. There is much to be said for a gatekeeper approach. It would permit a tempered[151] market experiment of competition between the more sophisticated universal model, on the one hand, and the simpler Internet banking and biller models, on the other hand. Thus, it would help reveal the strength of consumer preferences for the different models.[152] At the same time, it would provide the strongest assurance that consumers in fact would be protected from losses from fraud and error.

But the gatekeeper approach would do nothing to ensure the privacy of consumer information: it is feasible to require banks to hold deposit accounts unharmed from unauthorized transactions, but it is much more problematic to require them to ensure that intermediaries comply with their privacy obligations. A light scheme of federal regulation like the one discussed above could include monitoring of data-privacy compliance to assuage that concern. Moreover, for the reasons discussed above, the gatekeeper approach creates a substantial risk of anti-competitive conduct by banks

---

More specifically, even PayTrust has had some legal problems. For example, First Union Bank sued PayTrust arguing that its activities involved the unauthorized extraction of data from the bank's Web site, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The lawsuit reportedly settled after changes in some of PayTrust's practices. *See* Alan Charles Raul, *Protecting Factual Data* (June 2000) *at* http://www.sidley.com/cyberlaw/features/protecting_fd.asp (last visited Mar. 13, 2003). It is not clear, of course, whether that litigation reflects a failure of PayTrust to respect consumer privacy or an anticompetitive desire by First Union to exclude PayTrust from its accounts.

[150] *See, e.g.*, CheckFree 3-4 (discussing industry research suggesting the long-term superiority of that option); MURPHY REPORT, *supra* note 33, at 43.

[151] The experiment is tempered because of the dampening on competition inherent in the gatekeeper approach.

[152] One industry analyst argues cogently that the typical consumer eventually will come to use an aggregate site for most bills, and direct sites for a few important bills (such as a credit card) for which the consumer is more concerned about reviewing bill details. *See* MURPHY REPORT, *supra* note 33, at 43.

tempted to exclude their nonbank competitors. A separate federal regulatory apparatus would avoid that problem.

V. CONCLUSION

This paper is not an effort to write the last word on Internet payment intermediaries. Rather, it is an opening effort to explore the policy issues that the ongoing developments in the industry raise. The paper does not attempt to present a general discussion of those issues. For example, although disclosure obligations are central to the TILA and EFTA regimes, the paper does not address them – largely because I believe those obligations generally are pointless, if not actually harmful to consumers. Rather, the paper proceeds from the perspective that the most important regulatory issue relating to payment transactions is protecting consumers from fraud and error. Regarding the new transactions described in this paper, that concern is at great risk of being lost in the shuffle, primarily because money-laundering – an activity that does not directly harm consumers – is the central focus of regulatory attention.

Hoping to keep important consumer protections from being forgotten, the paper modestly calls for two steps of response. First, Part III suggests some minor updating to make the existing rules apply more coherently to the new transactions. The types of transactions that this paper discusses have reached a volume and level of stability that warrants adjustment of the regulatory regime. The basic premise of those adjustments is that consumers should not lose the protections they would have under conventional systems solely because they access those systems through a new Internet interface or intermediary. The need to allow experimentation among competing technologies does not require absolving those that conduct novel new payment transactions from the responsibilities that are customary for the conventional transactions conducted using the systems on which they rely.

Second, as discussed in Part IV, there are serious questions about the adequacy of the background framework that protects against abuses of the system either by those in the industry or by third parties attempting to take advantage of them. It certainly is important to give developing sectors of commerce an opportunity to stabilize before intervening by regulation that might freeze the industry's structure too soon. But there also is a substantial risk in waiting too long. Here, it is not at all clear that we know enough yet to make sensible decisions about the appropriate policy responses. The suggestions in Part IV are intended to be just that – illustrations of one way of resolving the various policy concerns based on one set of assumptions about the relevant facts and weight of the affected interests.

If anything, it is clear that a more informed decision could be made after a thorough study by a responsible entity of the federal government (such as the Federal Reserve), using its power to collect information from the industry. Such a study could provide an empirical sense of the significance of the problems that this paper discusses and develop a balanced solution that is sensitive to all the relevant interests.